Intel® Management and Security Status Application

User's Guide

January 2013

Document Revision Version: 1.0
Firmware version: 9.0

Intel Confidential

IMPORTANT—READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software or any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE—Subject to the restrictions below, Intel Corporation ("Intel") grants you the following limited, revocable, non-exclusive, non-assignable, royalty-free copyright licenses in the Software.

The Software may contain the software and other property of third party suppliers, some of which may be identified in, and licensed in accordance with, the various license files in the firmware kit.

DEVELOPER TOOLS—including developer documentation, installation or development utilities, and other materials, including documentation. You may use, modify and copy them internally for the purposes of using the Software as herein licensed, but you may not distribute all or any portion of them.

RESTRICTIONS—You will make reasonable efforts to discontinue use of the Software licensed hereunder upon Intel's release of an update, upgrade or new version of the Software.

You shall not reverse-assemble, reverse-compile, or otherwise reverse-engineer all or any portion of the Software.

Use of the Software is also subject to the following limitations:

You,

(i) are solely responsible to your customers for any update or support obligation or other liability which may arise from the distribution of your product(s)

(ii) shall not make any statement that your product is "certified," or that its performance is guaranteed in any way by Intel

(iii) shall not use Intel's name or trademarks to market your product without written permission

(iv) shall prohibit disassembly and reverse engineering, and

(v) shall indemnify, hold harmless, and defend Intel and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from your distribution of any product.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS—Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You will not remove, alter, deface or obscure any copyright notices in the Software. Intel may make changes to the Software or to items referenced therein at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY—If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES—EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel or its suppliers do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained in the Software.

LIMITATION OF LIABILITY—IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

Contents

Figures

1 *Introduction*

This *User's Guide* describes how to use the Intel® Management and Security Status application. The application's component tabs—detailed in this document—display information about a platform's support for the following technologies: Intel® Active Management Technology (Intel® AMT), Intel® Small Business Technology (Intel® SBT), Intel® Standard Manageability and Intel® Anti-Theft Technology (Intel® AT). All of these technologies are built upon the Intel® Management Engine (Intel® ME), a feature provided within the platform hardware.

The Intel® Management and Security Status icon indicates whether Intel® Active Management Technology, Intel® Small Business Technology, Intel® Standard Manageability and Intel® Anti-Theft Technology are running on the platform. The icon is located in the notification area. By default, each time Windows* starts, Intel® Management and Security Status application starts and the notification icon is displayed.

The Intel® Management and Security Status application has a separate version per every Intel® AMT generation (6.x, 7.x, 8.x, 9.x etc.). The installer for 9.x also supports the 8.x generation. If the Intel® Management and Security Status application starts automatically as a result of the user logging on to Windows*, the icon will be loaded to the notification area only if a supported combination of the following technologies is present on the platform: Intel® Active Management Technology, Intel® Small Business Technology, and Intel® Standard Manageability. If the Intel® Management and Security Status application is started manually (via the Start menu), the icon is loaded even if none of these technologies are enabled.

Note: The information displayed in the Intel® Management and Security Status application is not shown in real time. The data is refreshed at predefined intervals.

2 System Requirements

The Intel® Management and Security Status application has the following requirements:

- OS
    - Windows* 2003 Standard Edition R2
    - Windows* 2003 x64 EditionWindows* XP Pro with latest SP
    - Windows* XP x64 with latest SP
    - Windows* 7 Ultimate 32 bit with latest SP
    - Windows* 7 Enterprise 32 bit with latest SP
    - Windows* 7 Professional 32 bit with latest SP
    - Windows* 7 Ultimate 64 bit with latest SP
    - Windows* 7 Enterprise 64 bit with latest SP
    - Windows* 7 Professional 64 bit with latest SP
    - Windows* 7 Premium 64-bit with latest SP
    - Windows* 7 Home Premium 32 bit with latest SP
    - Windows* 7 Home Basic 32 bit with latest SP
    - Windows* 8
    - Windows Server *2008 x86 with latest SP
    - Windows Server *2008 x64 with latest SP
    - Windows Server* 2012
- Platform running Intel® Management Engine firmware
- Intel® Management Engine software installed

§

3 *Using the Intel® Management and Security Status Application and Icon*

Whenever either Intel® Active Management Technology, Intel® Small Business Technology or Intel® Standard Manageability is enabled, Intel® Management and Security Status icon is loaded into the notification area when Windows* starts. It can also be started by clicking **Start> All Programs\Intel\Intel® Management and Security Status\ Intel® Management and Security Status**.

While the Intel® Management and Security Status application is running, the Intel® Management and Security Status icon is visible in the notification area. This icon will appear blue if any one of the aforementioned technologies is enabled on the computer. In any other case, the icon will appear gray.

Note: The icon will also be gray if the Intel® Management and Security Application User Notification Service is not running or the Intel® Management Engine Interface (Intel® MEI) driver is disabled or unavailable.

To view the Intel® Management and Security Status application:

- Double-click the Intel**®** Management and Security Status icon, or

- Right-click or left-click the icon and choose **Open**, or

- Click **Start>All Programs>Intel>Intel® Management and Security Status> Intel® Management and Security Status**.

Note: If your computer is set to Classic Start Menu, the path will start with 'Programs' instead of 'All Programs'.

The following sections describe the information available in the application's tabs. Information about the application is available also by clicking either the "Learn more" button   or link.

Note: The application dynamically hides tabs that are not relevant. For example, on platforms that do not support Intel® AT, the Intel® AT tab is hidden.

3.1 General Tab

The **General** tab provides status information about the Intel AMT, Intel SBT, Intel®
Standard Manageability, and Intel AT status, and events related to these technologies.

Figure 3-1.
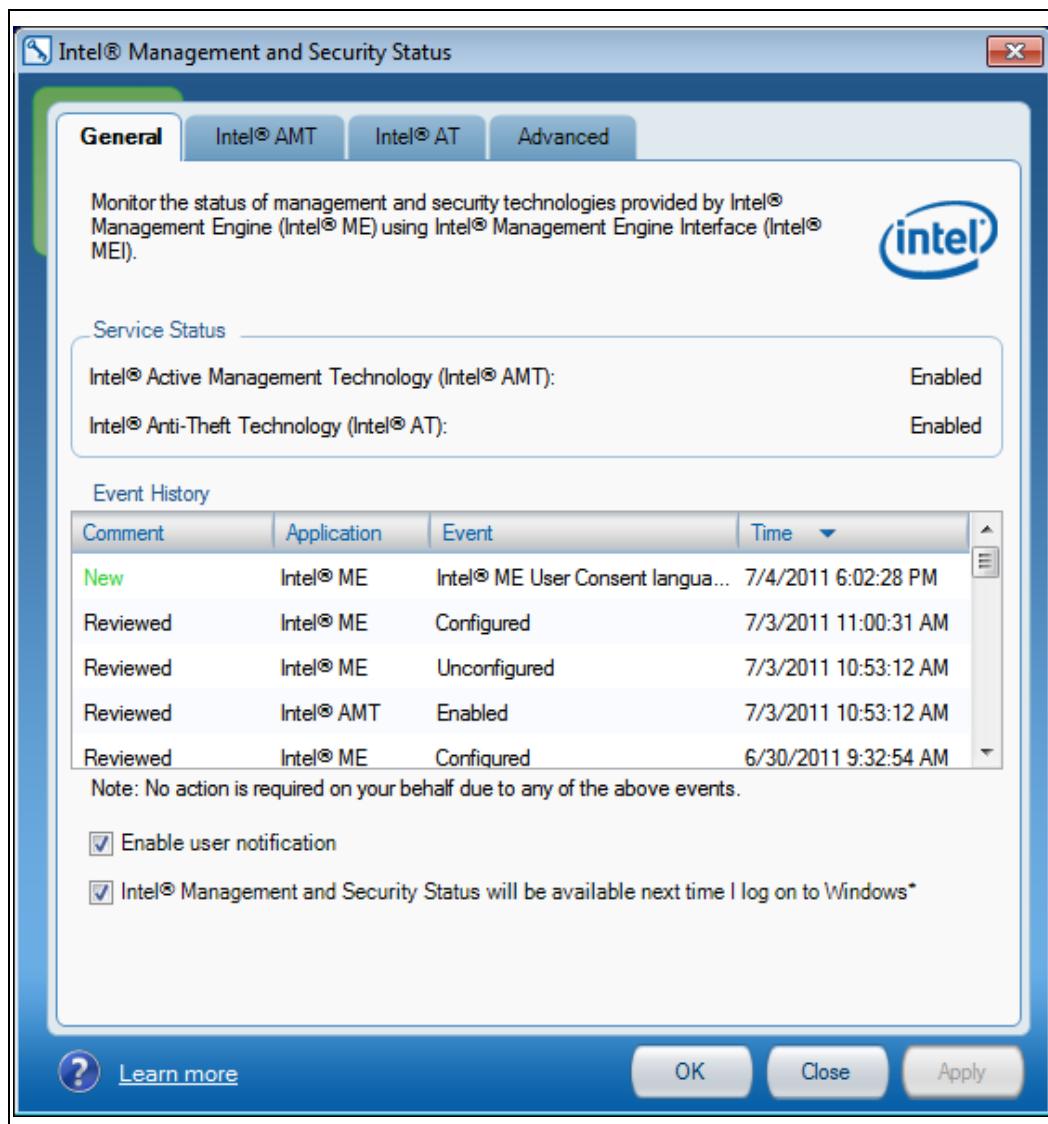
Events and some of their details are displayed in the **Event History** section. These can be sorted by clicking on the relevant column header.

The status of Intel® Active Management Technology, Intel® Small Business Technology, Intel® Standard Manageability or Intel® Anti-Theft Technology is displayed in the **Service Status** section depending on which technology is operational on the system. The tab displays information for Intel® Active Management Technology, Intel® Small Business Technology, or Intel® Standard Manageability. The status can be one of the following:

- **Intel® AMT**: Enabled / Disabled / Information unavailable

  - When Intel® AMT status presents Enabled it means that the Intel® AMT is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Intel® AMT is functional and operating).

  - When Intel® AMT status presents Disabled it means that the Intel® AMT is either not enabled on the system or has been disabled by the IT administrator.

  - Information unavailable: It is not known whether Intel® AMT is supported on the system. No Intel® AMT information is available. This can be for one of the following reasons: LMS service has stopped, or the Intel® Management Engine Interface (Intel® MEI) driver is disabled.

- **Intel® SBT**: Enabled / Disabled / Information unavailable

  - When Intel® SBT status presents Enabled it means that the Intel® SBT is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Intel® SBT is functional and operating).

  - When Intel® SBT status presents Disabled it means that the Intel® SBT is either not enabled on the system or has been disabled by the IT administrator.

  - Information unavailable: It is not known whether Intel® SBT is supported on the system. No Intel® SBT information is available. This can be for one of the following reasons: LMS service has stopped, or the Intel MEI driver is disabled.

- **Intel® Standard Manageability**: Enabled / Disabled / Information unavailable

  - When Intel® Standard Manageability status presents Enabled it means that the Intel® Standard Manageability technology is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Intel® Standard Manageability is functional and operating).

  - When Intel® Standard Manageability status presents Disabled it means that the Intel® Standard Manageability technology is either not enabled on the system or has been disabled by the IT administrator.

- Information unavailable: It is not known whether Intel® Standard Manageability technology is supported on the system. No Intel® Standard Manageability information is available. This can be for one of the following reasons: LMS service has stopped, or the Intel MEI driver is disabled.

- **Intel® Anti-Theft Technology**: Enabled. This means that the Intel® Anti-Theft Technology feature is supported on the platform. If Intel® Anti-Theft Technology is not supported on the platform; no reference to it is displayed. The feature becomes activated only after the platform has been enrolled with an Intel® Anti-Theft Technology service provider and all required configurations have been applied.

Note: The information in this field shows the state of the platform at the last platform boot.

Enable user notification: Checking this box allows the user to enable or disable the Intel® Management and Security Status icon from displaying important notifications in the notification area (for instance, notification will be sent when one of the technologies is enabled or disabled). Checking or unchecking the checkbox affects the Intel® Management and Security Status application setting for the current user account only.

On Windows* 8 platforms, IMSS user notifications are also displayed as Windows* 8 UI 'Toast' notifications, visible to users working with the Windows* 8 UI. These notifications will only be displayed as long as a Windows* 8 UI Start Menu shortcut (Windows* 8 UI 'tile') is present.

Intel® Management and Security Status application will be available next time I log on to Windows*: Checking this box causes the Intel® Management and Security Status application to be invoked, and the icon to be displayed, whenever you log on to Windows*. Checking or unchecking the checkbox affects Intel® Management and Security Status application's behavior for the current user account only.

Note: The application does not load automatically with Windows* log-on if none of the technologies it displays (Intel® Active Management Technology, Intel® Small Business Technology or Intel® Standard Manageability) are supported on the platform. Intel® Management and Security Status application will load automatically even if all of the technologies are disabled, so long as they are supported. Intel® Management and Security Status application will not load if these technologies are not supported in the platform.

3.2 Intel® Active Management Technology Tab

Note: This tab is displayed only if the platform supports Intel® AMT.

Click the **Intel® AMT** tab to display Intel® AMT information.

Figure 3-2.
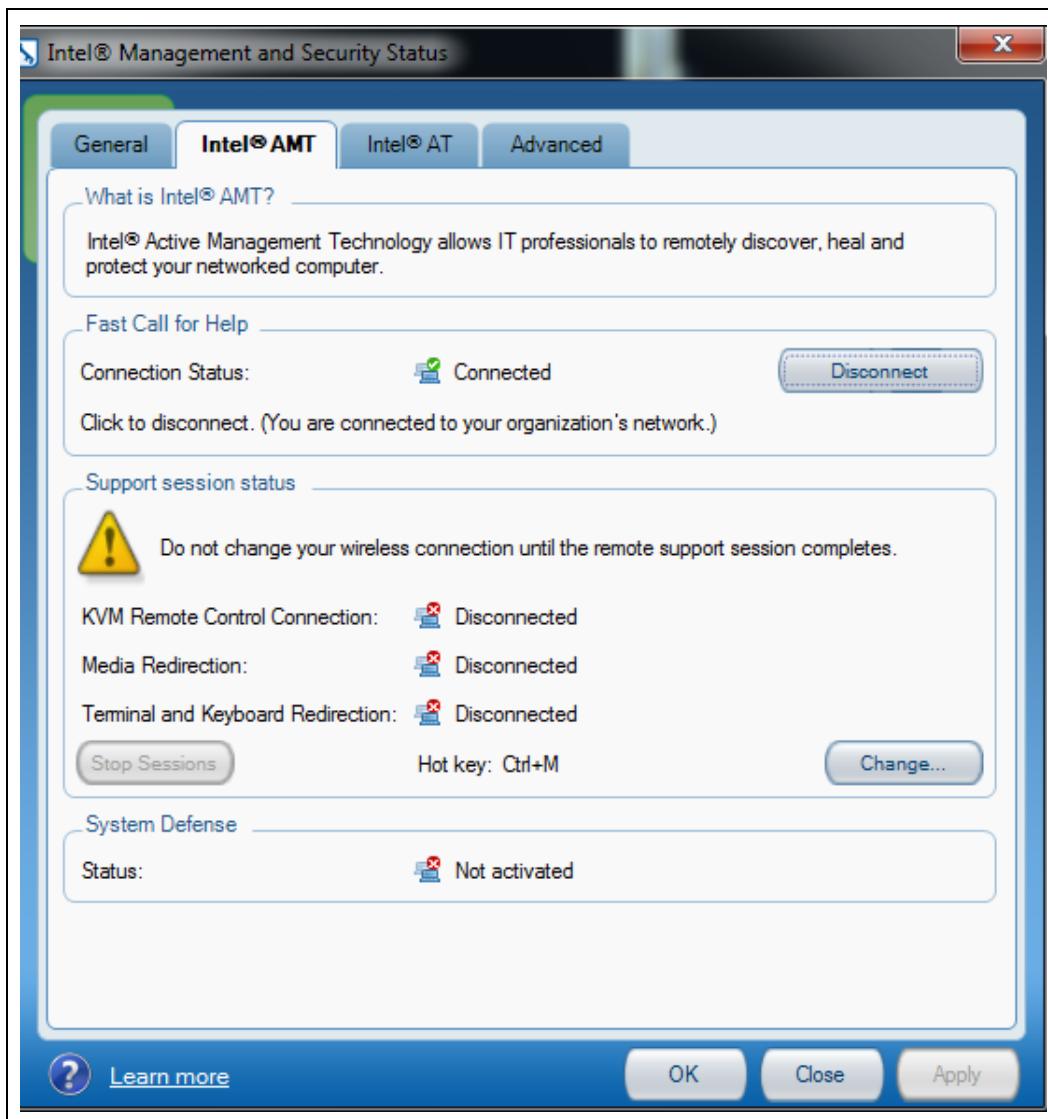
3.2.1 Fast Call for Help

The Fast Call for Help section provides Client Initiated Local Access (CILA) or Client Initiated Remote Access (CIRA) capabilities depending on whether the system is connected to the corporate network or not, respectively. The Fast Call for Help section will be available for the CIRA/CILA use-cases, providing the proper configuration for CIRA/CILA has been done, as well as for a case in which the user's system did not receive an IP address while the wireless network is available for a support session to take place. Otherwise, the Fast Call for Help section will be grayed out.

CIRA allows a user to connect the Intel® AMT system to the company's Information Technology network from an external internet connection. Click the "Get Technical Help" button to connect to your Information Technology network for system diagnostics and maintenance. The current connection status is displayed in this section as well.

CILA (Client Initiated Local Access) feature allows a user connected to the internal corporate network to send a support request to the IT administrator.

Note: In order for CIRA/CILA to work, the machine needs to be configured correctly, and support this technology. Such settings are typically done by management software. (Configuration details appear in the Intel® AMT SDK Implementation and Reference Guide).

Note: The information displayed in the Intel® Management and Security Status application, including the Fast Call for Help section, is not shown in real time. The data is refreshed every time an event has arrived.

Note: When the user is connected as Guest account (in Windows*) the "Fast Call For Help" section will be grayed out. This was designed to prevent users outside of the organization to influence the organization network.

3.2.2 Support Session Status

The following information is provided:

- **KVM Remote Control Connection**

  Indicates whether KVM (Keyboard, Video & Mouse) Remote Control session is open.
  Possible values: Connected/ Disconnected/ Information unavailable.
  The "KVM Remote Control Connection" section will be grayed out if the KVM Remote Control feature is disabled on the system.

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

- **Terminal and Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

- **Stop Sessions**

  Click the "Stop Sessions" button to close any open KVM Remote Control, media redirection, or terminal/keyboard redirection sessions. In cases when user consent is required for such a session, re-establishing the session will require renewal of user consent after clicking this button.

- **Hot Key**

  Indicates the hot key which could be used to close any open KVM Remote Control, media redirection, or terminal/keyboard redirection sessions (same effect as "Stop Sessions" button).

  Click on the "Change" button to choose a different hot key for terminating an open session.

- **Prevent Access**

  This button will appear in cases where user consent is required for a remote support session to occur. In such cases, after the user will provide the required approval to the remote administrator and as long as the healing session hasn't begun, the user will see the "Prevent Access" button. This button enables the user to change his/her mind, as clicking on it will cancel user consent and disable the ability of the IT administrator to begin the remote session. During this time, the Hot Key will also serve as a means to cancel user consent. Once a remote support session has begun, the "Prevent Access" button will no longer be visible, and the "Stop Sessions" button will appear instead.

Note: User Consent, when required, will be granted to the administrator per session, by the user giving the administrator a one-time pass code which will appear on the Secure Output Window presented on the user's screen. See more about Secure Output Window and User Consent Policy under Advanced Tab - Secure Output Window Settings.

Note: During a Support Session conducted over the wireless interface, a notice will be displayed with a warning triangle. The message will say: "Do not change your wireless connection until the remote support session completes".

Intel® Management and Security Status Application Icon during support session

- The notification area tray icon appears animated as long as user consent or support session is active.

- Stop Sessions/ Prevent Access are available also thru clicking on the tray icon.

Intel® AMT tab view with "Prevent Access" button enabled:

Figure 3-3.
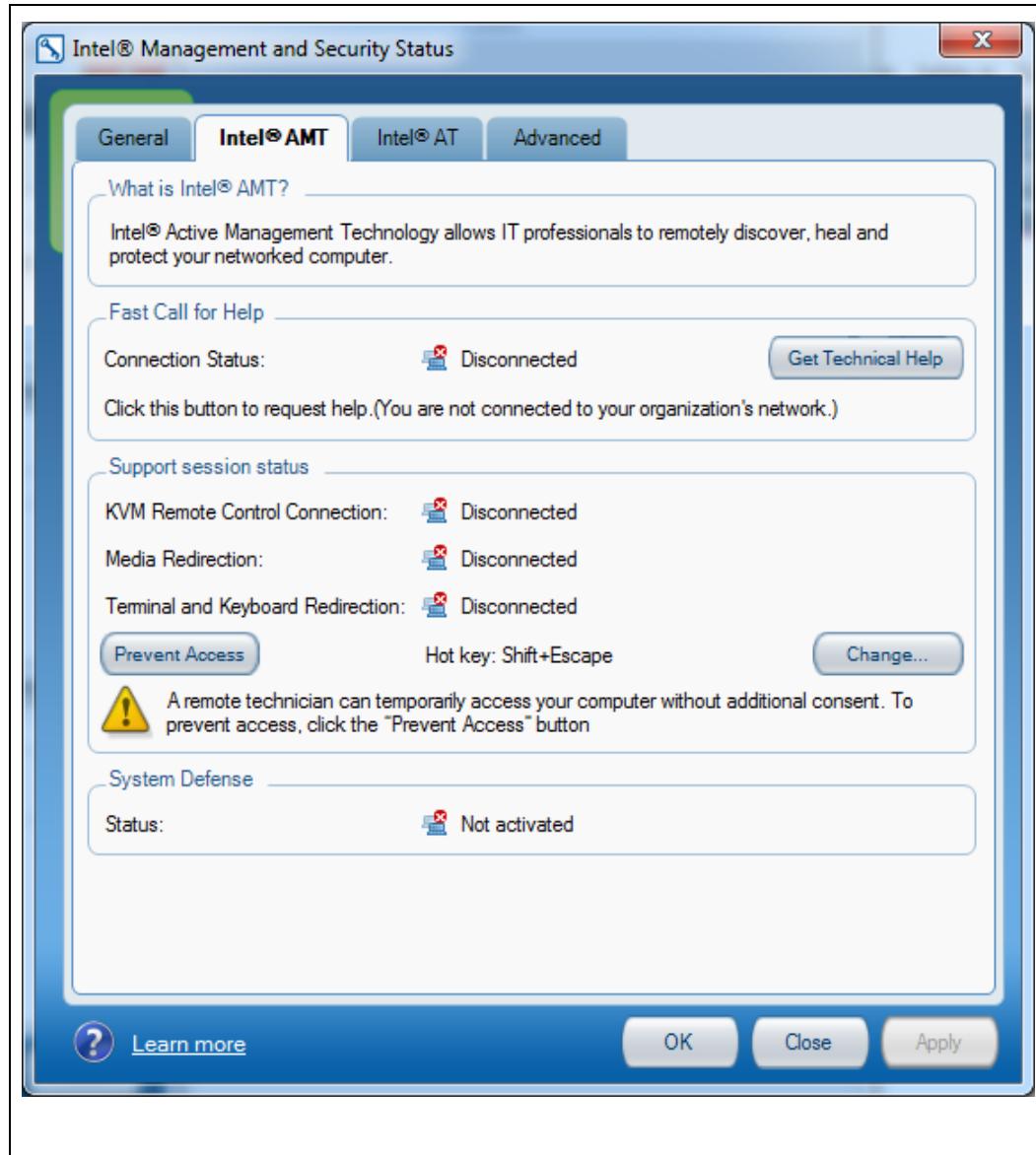
3.2.3   System Defense

- **System Defense Status**

  Indicates whether System Defense policies are currently active.
  Possible values: Activated/Not activated/ Information unavailable.

3.3 Intel® Small Business Technology Tab

Note: This tab is displayed only if the platform supports Intel® Small Business Technology (Intel® SBT).

Click the **Intel® SBT** tab to display Intel® SBT information.

Figure 3-4.
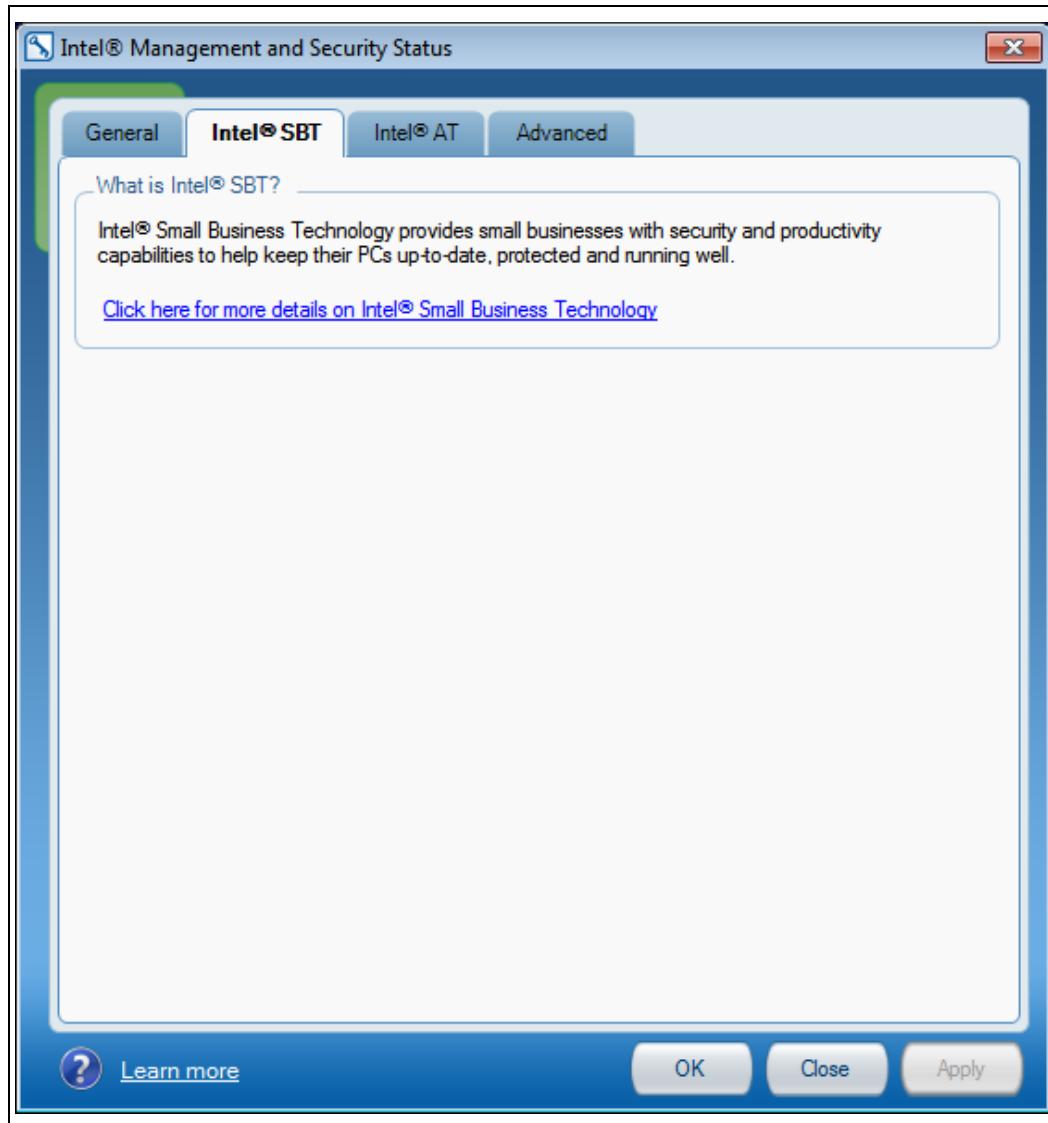
Clicking the link in the **What is Intel® SBT** section connects you to an Intel site that provides you with information about Intel® Small Business Technology.

3.4 Intel® Standard Manageability Tab

Note: This tab is displayed only if the platform supports Intel® Standard Manageability.

Click the **Intel® Std Mgt** tab to display Intel® Standard Manageability information.

Figure 3-5.
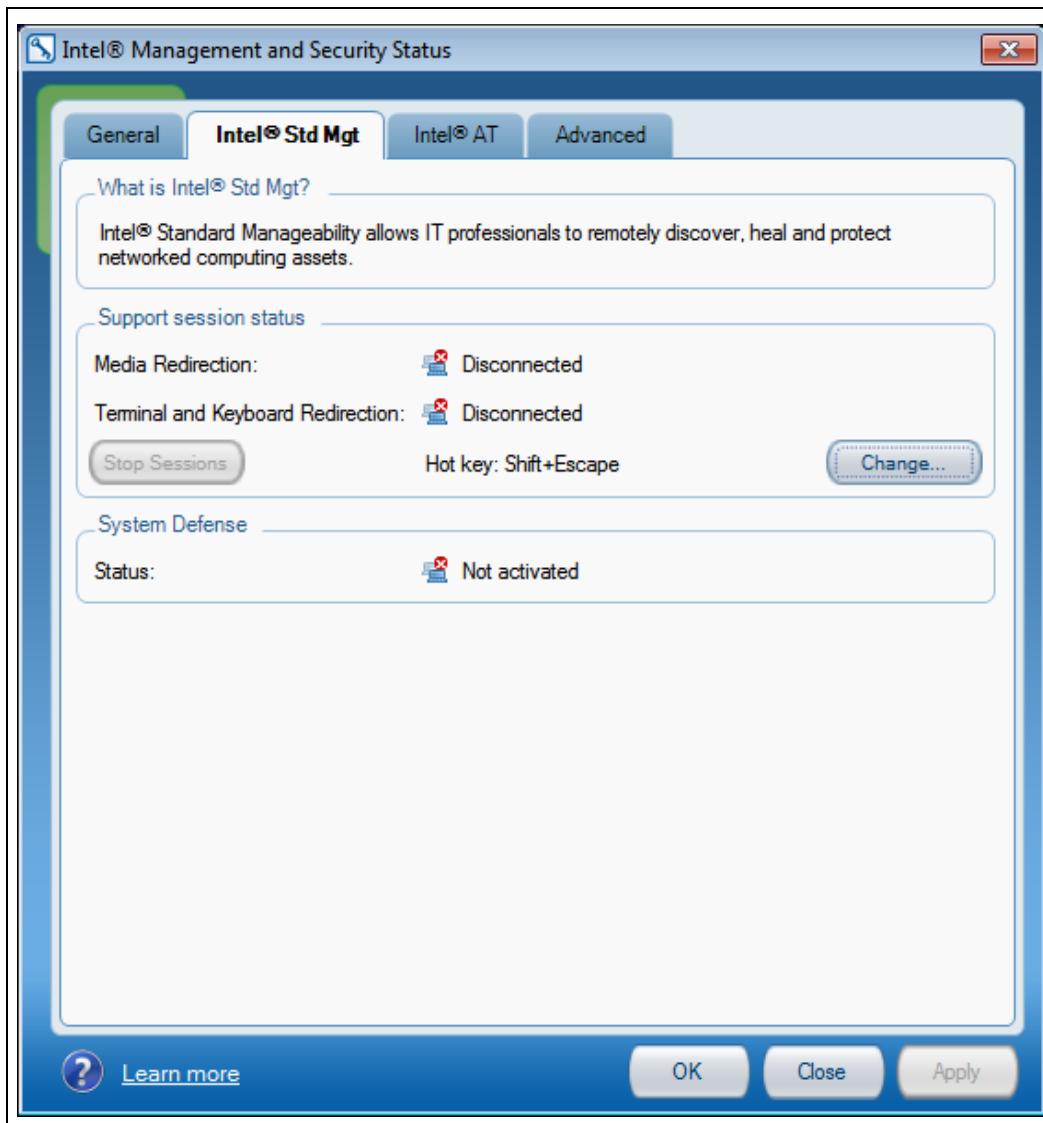
3.4.1 Support Session Status Section

The following information is provided:

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable

- **Terminal and Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

3.4.2 System Defense

- **System Defense Status**

  Indicates whether System Defense policies are currently active.
  Possible values: Activated/Not activated/ Information unavailable.

3.5 Intel® Anti-Theft Technology Tab

Note: This tab is displayed only if the platform supports Intel® AT.

Click the Intel® AT tab to view Intel® Anti-Theft Technology information.

Note: The information in this tab shows the state of the platform when it was last booted.

Figure 3-6.
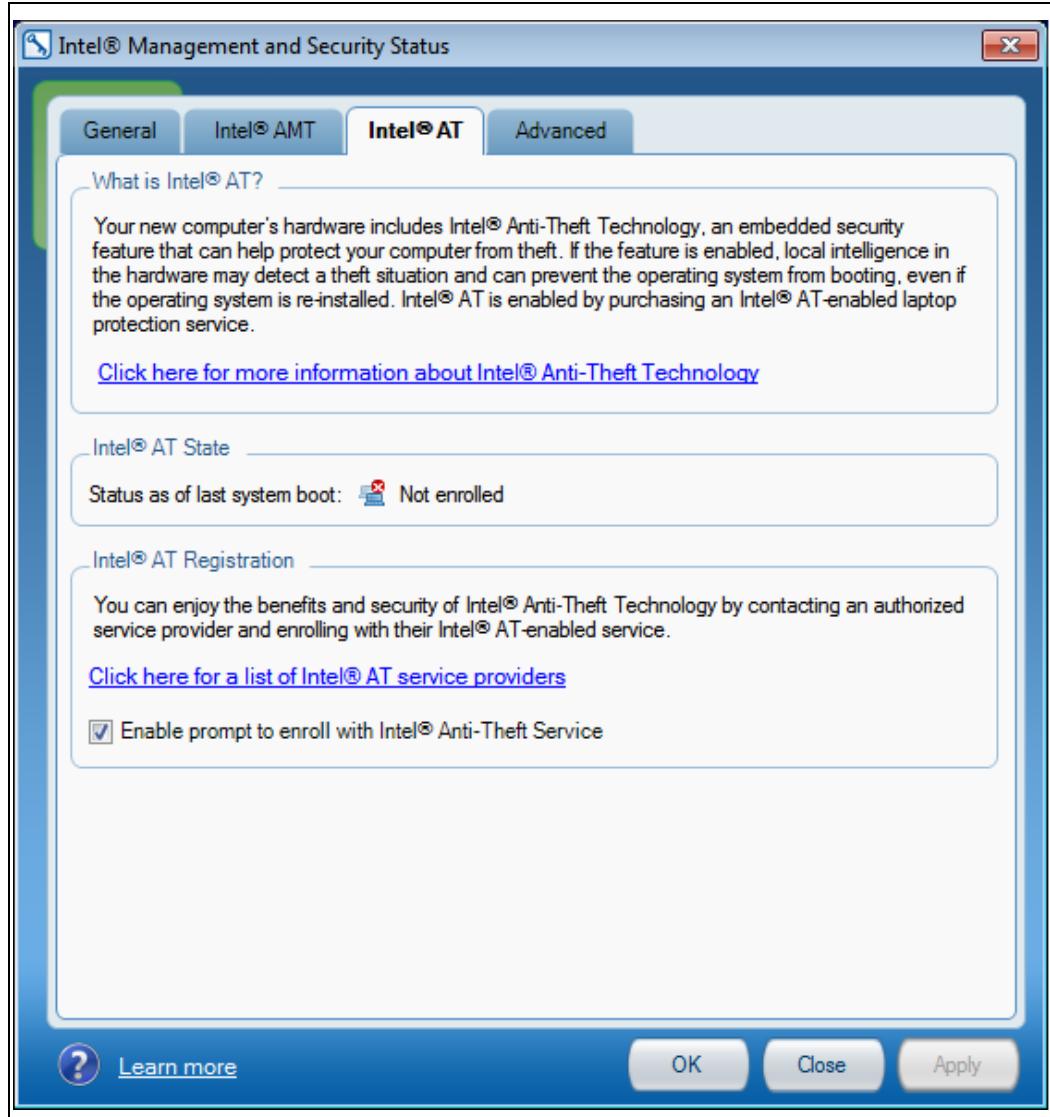
Clicking the link in the **What is Intel® AT** section connects you to an Intel site that provides you with information about Intel® Anti-Theft technology.

3.5.1   Intel® AT State

Provides the following information:

Enrolled: The platform has been enrolled with a service provider that is providing Intel® Anti-Theft Technology protection for it.

Not Enrolled: The platform has not been enrolled with a service provider that is providing Intel® Anti-Theft Technology protection.

3.5.2 Intel® AT Registration

Note: This section is displayed only if the platform has not been enrolled with a service provider that is providing Intel® Anti-Theft Technology protection.

Clicking the link in this section displays a list of Intel® AT service providers in your area and allows you to enroll with their Intel® AT service.

**Enable prompt to enroll with Intel® Anti-Theft Technology Service:** If this box is checked, a balloon displaying an invitation to enroll with Intel® AT service is displayed every 5th time that the Intel® Management and Security Status application is started. If the platform has been enrolled with Intel® AT service, the balloon is not displyed.

3.6 Advanced Tab

Click the **Advanced** tab to view additional information.

Note: The image below includes all buttons and information that may be displayed by Advanced Tab. However, not everything will be displayed at all times, as this depends on the specific technologies which are enabled and active on the platform (Intel® Active Management Technology (Intel® AMT), Intel® Small Business Technology (Intel® SBT) or Intel® Standard Manageability).

Figure 3-7.
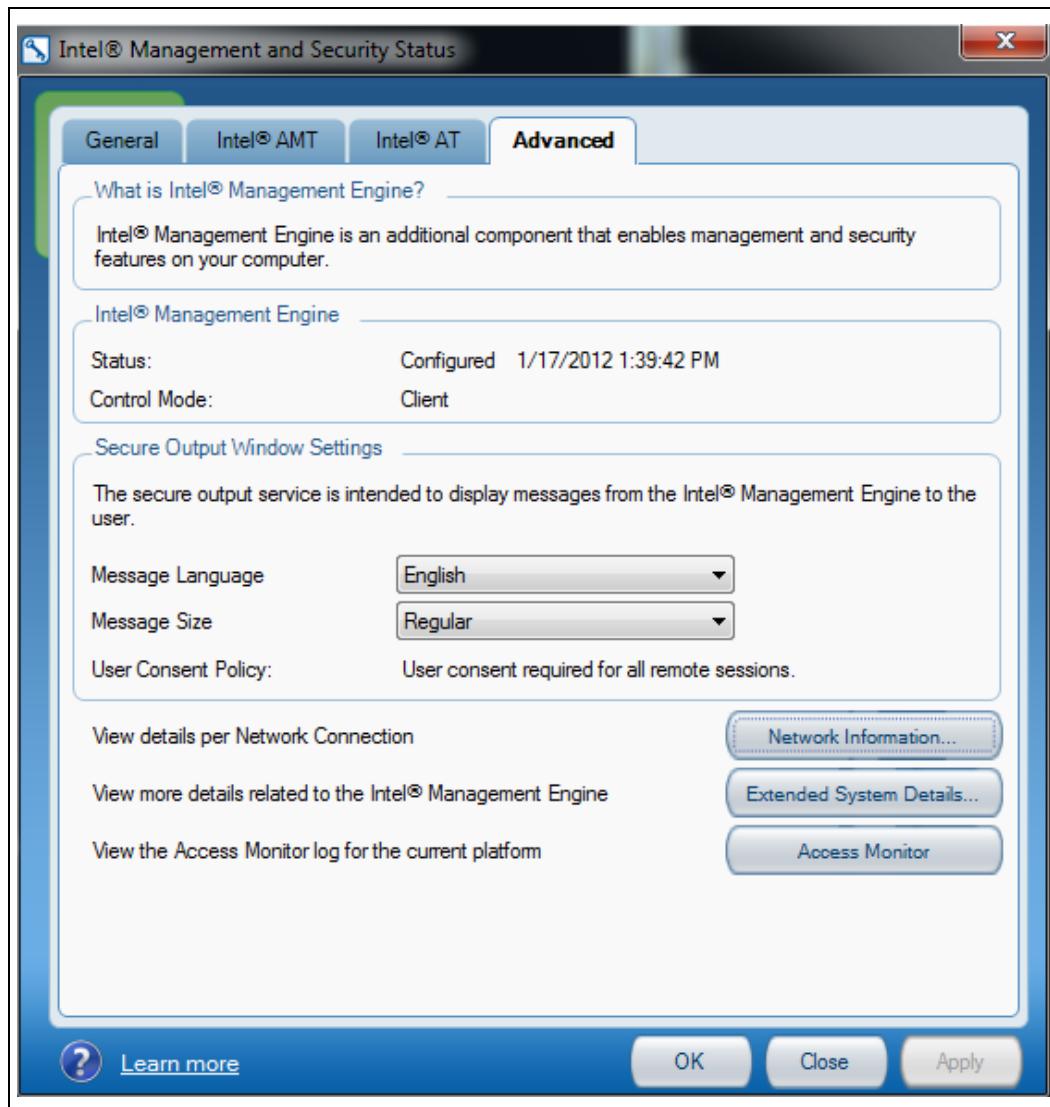
3.6.1 Intel® Management Engine

The following information is provided:

- **Status**

  The operational status of Intel® ME
  Possible values: Configured / Unconfigured / Information unavailable.
  In case status is Configured, the configuration date and time will be displayed.

- **Control Mode**

  There are two configuration modes for Intel® ME – Client Control Mode and Admin Control Mode. If status is Configured, the relevant Control Mode will be shown.

3.6.2 Secure Output Window Settings

The following information is provided for the Secure Output feature, implemented in KVM (keyboard/video/mouse) redirection. If the machine was configured in Client Control Mode this is provided in IDE redirection and remote power operations as well.

- **Message Language**

  Specifies the language used by the Secure Output feature for user consent. Choose one of the listed languages.

  Upon installation of the Intel® Management and Security Status application, the consent language will be set according to the Windows* System Locale language (note that this may be different than the Windows* Display language). Selecting a different Message Language on the Advanced Tab will override this initial setting. Selecting "Windows Default Language" will revert to the Windows* System Locale language.

Note: On Windows* XP, Chinese characters may appear as rectangles and Hebrew and Arabic may appear reversed, if the relevant language packs have not been installed. Windows* XP does not include all language packs by default. They can be added through the "Control Panel." Open "Regional and Language Options," then click the languages tab. Under "Supplemental Language Support" select the extra languages you wish to install, and follow the instructions.

- **Message Size**

  Specifies the window size of messages displayed by the Secure Output Feature. Choose one of the following: **Regular** or **Large**. **User Consent Policy**

  Specifies the policy for when the user's approval will be required in order to establish a remote support session by an IT administrator. User Consent will be granted to the administrator per session, by the user giving the administrator a one-time pass code which will appear on the Secure Output Window presented on the user's screen.

- **Possible Policies are:**

  User consent not required for any remote session

  User consent required for KVM session only

  User consent required for all remote sessions (i.e., KVM, IDE redirection, and remote power operation)

3.6.3   WLAN Control

On Intel ME 8.0 systems only, the WLAN control section appears when there is an active support session in which the remote IT administrator is connecting to the user's machine via wireless network.

This section is not shown on platforms from Intel ME 8.1 onwards.

- **Restore Connection button**

    On Intel ME 8.0 systems only, if the remote administrator begins a support session using the wireless network, there is temporarily no wireless network available to the user's Operating System. The Restore Connection button enables the user to return control of the wireless network to the OS. However, if this button is clicked while the remote support session is still active, the session will be terminated.

    This button is not shown on platforms from Intel ME 8.1 onwards.

3.6.4   Network Information

Click the "Network Information" button to display network details regarding Intel® ME wireless and wired connectivity.

Figure 3-8.
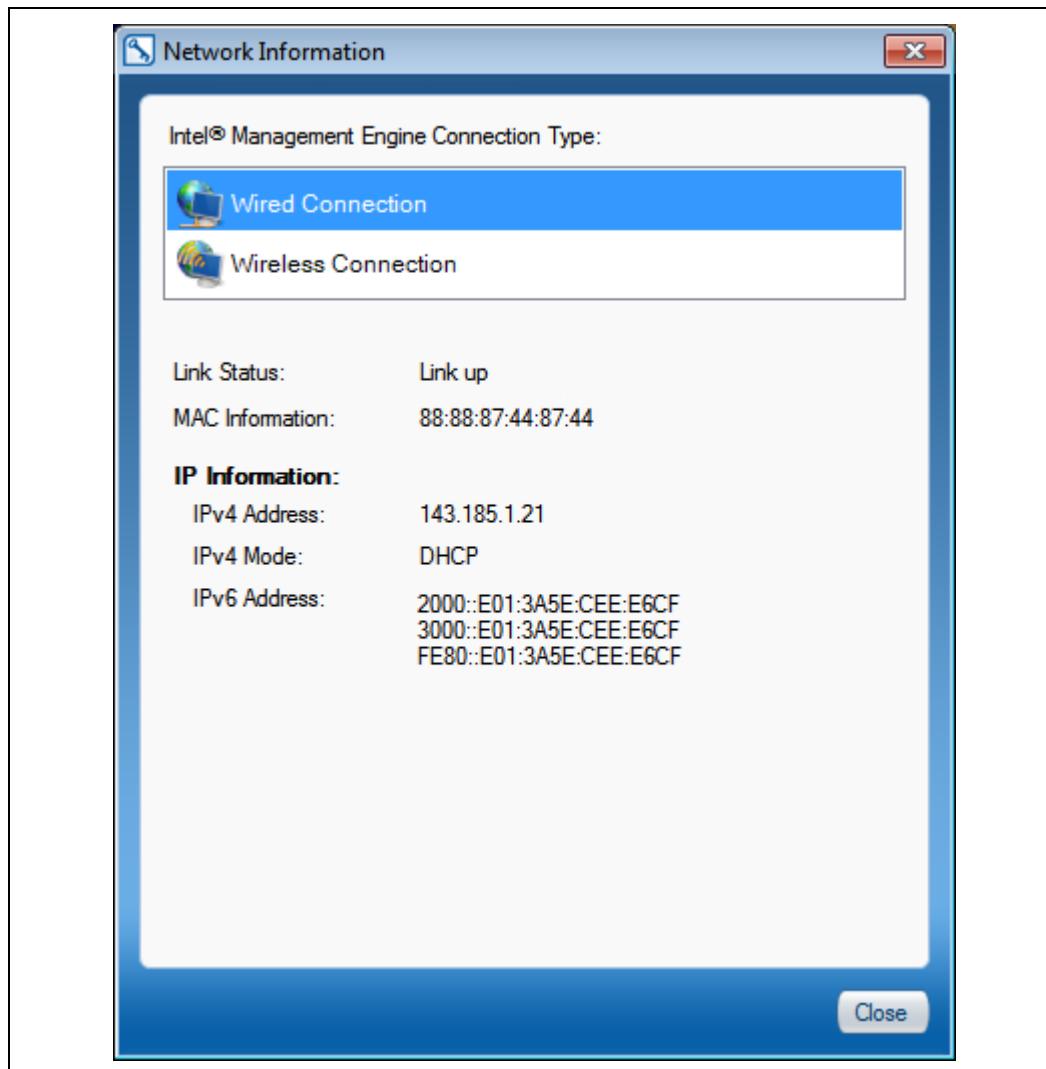
In the **Connection Type** section, click either **Wireless Connection** or **Wired Connection** to display information on the following items for the selected interface:

- **Link Status**

  Whether the link is currently active.
  Possible values are: Link up/Link down/Information unavailable

- **MAC Information**

  XX:XX:XX:XX:XX:XX – e.g. 88:88:88:0A:88:87

Intel Confidential

- **IPv4 Address**

  XXX.XXX.XXX.XXX – e.g. 208.77.188.166

- **IPv4 Mode**

  Possible values: Static/ DHCP/ Information unavailable.

- **IPv6 address**

  If IPv6 addressing is enabled for the Intel ME, the Intel® Management and Security Status application displays up to 6 IPv6 IP addresses configured for an Intel ME network interface for wired connection, and up to 5 IPv6 IP addresses for wireless connection.

Figure 3-9.
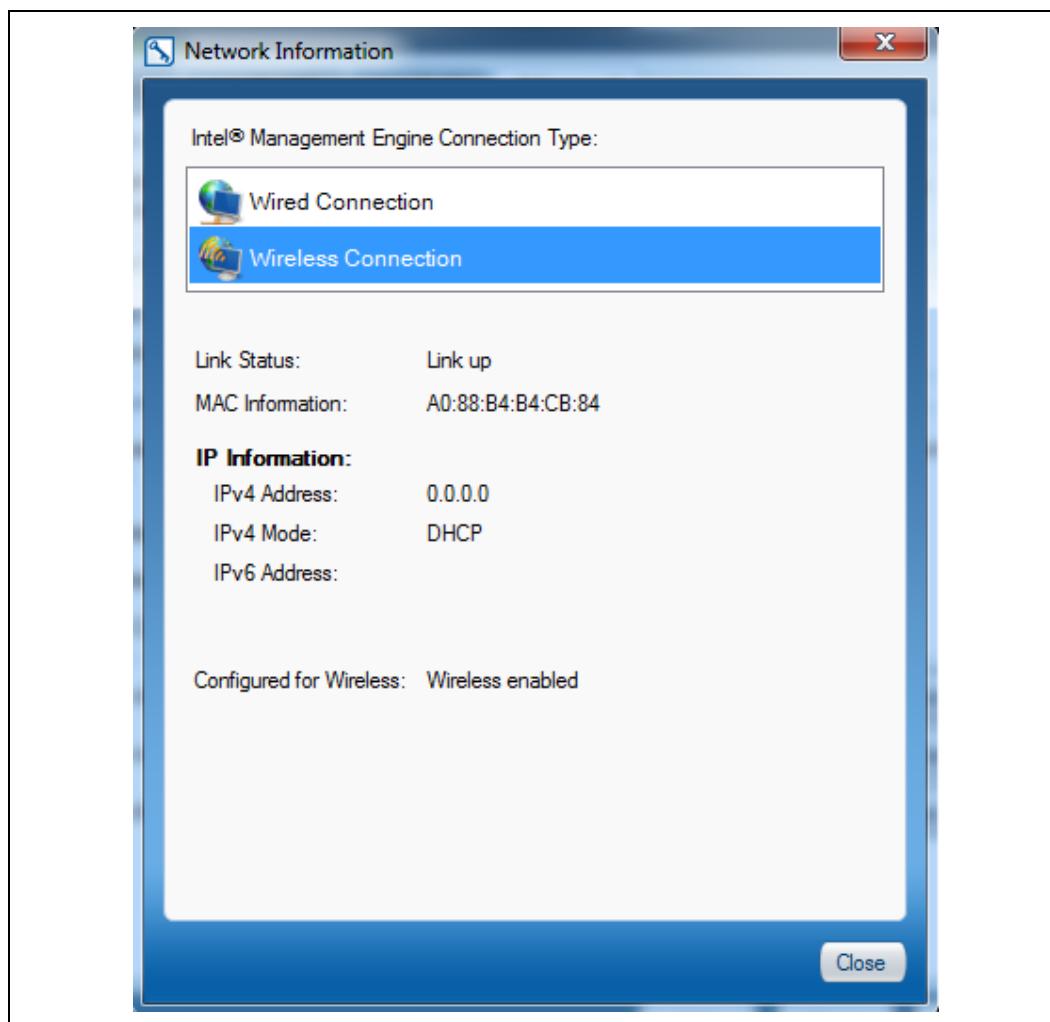
<u>Data which appears only for Wireless Connection</u>

- **Configured for Wireless**

  Possible values are: Wireless enabled/ Wireless disabled/ Information unavailable.

- **WLAN control**

  On Intel ME 8.0 systems only, the WLAN control indicates whether the wireless network is available to the user's computer operating system (i.e. regular usage) or whether it is in control of the Intel® Management Engine for the purpose of remote support by an IT administrator. Possible values are: HOST / Intel® ME. This control is not shown on platforms from Intel ME 8.1 onwards.

- **WLAN preference**

  On Intel ME 8.0 systems only, WLAN preference indicates whether the wireless network should preferably be in control of the operating system or the Intel® Management Engine (Intel® ME). Expected behavior is for WLAN control to be the same as WLAN preference. However, if for some reason the operating system fails to take control over the wireless network (e.g. the wireless driver is dysfunctional), the user will witness WLAN preference given to the operating system while WLAN control is with Intel® ME (even if the Return Control button was clicked). Possible values are: Operating System/ Intel® ME. This control is not shown on platforms from Intel ME 8.1 onwards.

3.6.5   Extended System Details

When clicking Extended System Details, a Windows* System Information window will open, providing an extensive report about system components and configuration.

The report includes both general information regarding the system ("Host Information") and specific Intel® Management Engine Information ("Intel® ME Information").

It is possible to save the system report to a file by clicking File->Export on the System Information Window.

Below are explanations for some of the details displayed under Intel® ME Information:

Host information:

- Operating System Name – The Windows* operating system that the application is running on.

- Operating System Version – The version of the operating system.

- System Manufacturer – The hardware manufacturer.

- System Name – The computer name as recognized by the operating system.

- System Model – The hardware platform name.

- Processor – The processor full brand name.

- BIOS Version – The BIOS manufacturer name and BIOS version number.

- LAN Driver – The version number of the LAN device driver.

- LAN DeviceID – The PCI Device ID for the LAN device.

- WLAN Driver - The version number of the Wireless LAN device driver.

- WLAN DeviceID – The PCI Device ID for the Wireless LAN device.

Intel® ME Information:

- Intel ME Control Mode – The configuration mode (Client Control or Admin Control).

- Provisioning Mode – State of Intel ME configuration (Pre/In/Post).

- BIOS boot – The BIOS boot state (expected to be Post Boot).

- Last Intel ME reset reason - The reason that the Intel® ME was last reset (Global System/ FW reset / Power Up/ Unknown cause/ Information unavailable).

- System UUID – The Universal Unique Identifier of the computer. Standard System UUID presentation, such as: 03000200-0400-0500-0006-000700080009.

- Local FWUpdate – The local firmware update policy (Enabled/Disabled).

- Power Policy – The power modes in which Intel® ME is available (ON in S0 or Intel ME ON in S0/S4/S5/DC). Note: S0 = Power is on, S4 = Hibernate, S5 = System is shut down though power cable is connected, DC = Battery Power.

- Cryptography Support – The Intel® ME capability to work in TLS/SSL mode (Enabled/Disabled).

FW Capabilities:

Indicates whether the following technologies are present on the platform and enabled:

Intel® Active Management Technology / Intel® Standard Manageability / Intel® Small Business Technology

Intel® Anti-Theft Technology PC Protection

Intel Capability Licensing Service

Intel® ME Dynamic Application Loader

Protect Audio Video Path

Intel® Active Management Technology / Intel® Standard Manageability / Intel® Small Business Technology

Technology State (Enabled or Disabled).

Technology Status (Configured/Not Configured).

CIRA Connection Status – Client Initiated Remote Access Connected/Disconnected (not available for Intel® Standard Manageability and Intel® Small Business Technology).

Intel® AT

Intel® AT State (Enabled or Disabled).

Intel® AT Status (Enrolled or Not Enrolled).

Components Information

Presents versions for the following components:

- MEBx Version - Intel® ME BIOS Extension version.
- FW Version – Firmware version.
- LMS Version – Local Management Service software version.
- Intel MEI Driver Version – Intel® Management Engine Interface driver version.
- Intel MEI DeviceID – Intel® Management Engine Interface PCI Device identification.
- SOL Driver Version – Serial Over LAN driver version.
- SOL DeviceID - Serial Over LAN PCI Device identification.

Network Information:

- LAN MAC Address **–** The Media Access Control address for the LAN device.
- LAN Configuration state – DHCP or static mode for LAN.
- LAN Link Status – LAN link up or down.
- LAN IPv4 Address **–** The IPv4 address assigned to LAN.
- LAN IPv6 Enablement – IPv6 enabled or disabled for LAN.
- WLAN MAC Address **–** The Media Access Control address for the Wireless LAN device.
- WLAN Configuration state – only DHCP mode supported for Wireless LAN.
- WLAN Link Status – Wireless LAN link up or down.
- WLAN IPv4 Address **–** The IPv4 address assigned to Wireless LAN.
- WLAN IPv6 Enablement – IPv6 enabled or disabled for Wireless LAN.

Note: When the user is connected as Guest account (in Windows*), some of the system information will not be available. In such a case, all Host Information and some of the Intel® ME Information (such as Software Versions) will appear as "NA".

3.6.6   Access Monitor

If the Access Monitor feature is enabled on the platform, then by clicking the "Access Monitor" button, the relevant content will be presented through a Windows* System Information window which will then open. Access Monitor content includes description of events which occurred on the system and may be of interest to the user from a privacy and security perspective, such as Network Administration, Storage Administration, Remote control Operations and more.

Note: Events that occurred before first provisioning of Intel® AMT or Intel® SBT will appear with irrelevant time/date.

3.6.7   Advanced Tab with Intel® SBT

Intel® Small Business Technology does not support remote management, therefore in the case of an Intel® SBT system, the Advanced Tab will be limited to the following:

Figure 3-10
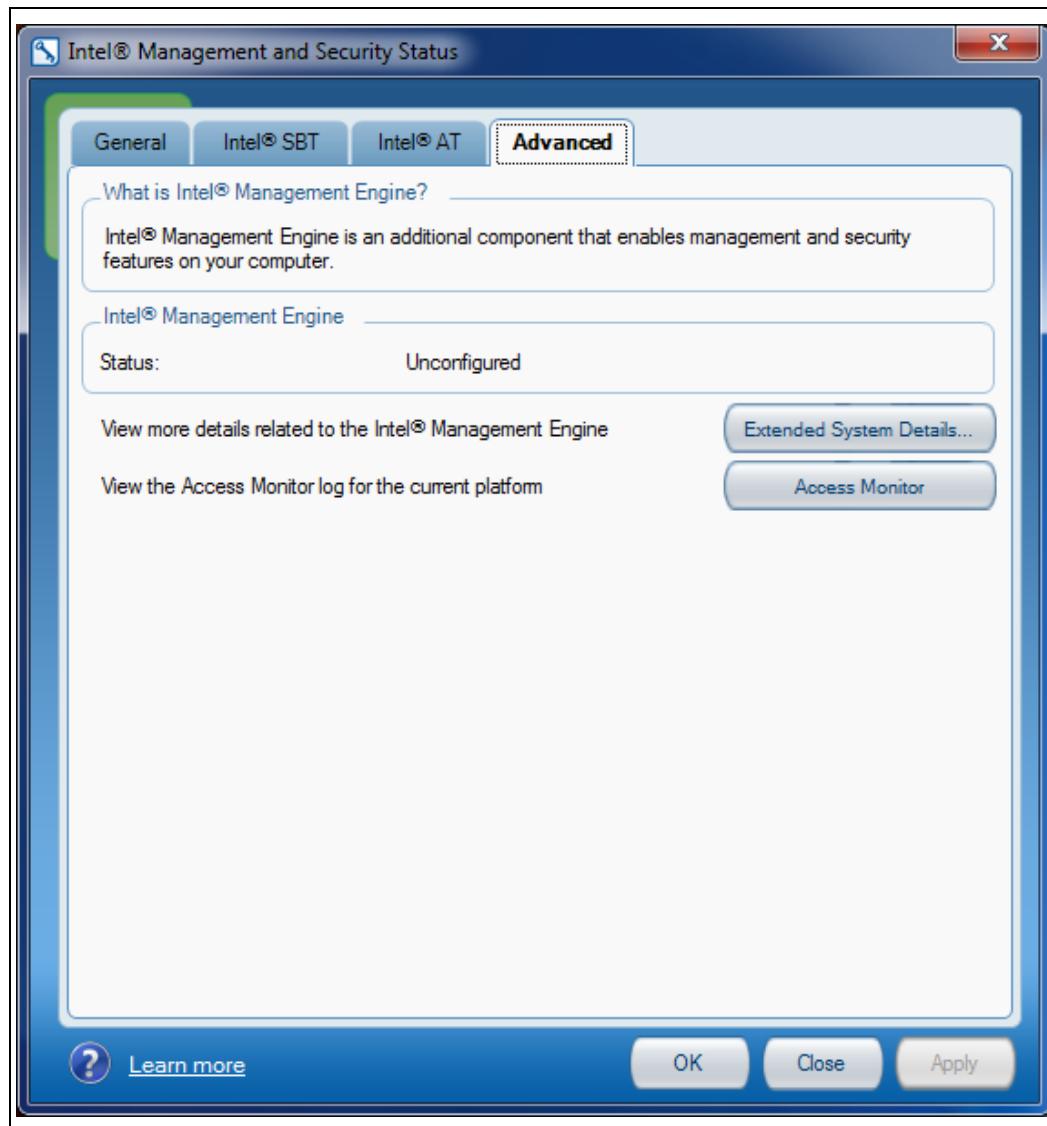
3.7 Exiting the Application

To exit the application, right click or left click on the Intel® Management and Security Status application icon in the notification area and select **Exit**.

The following window is displayed.

Figure 3-11
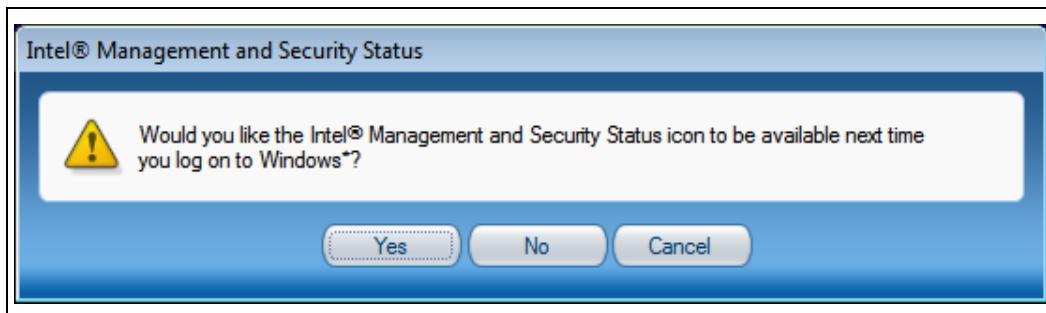
- Click **Yes** to automatically start the Intel® Management and Security Status application when you next log on. (**Note:** this change affects Intel® Management and Security Status application behavior for the current user account only).

- Click **No** to not start the Intel® Management and Security Status application when you next log on. (**Note:** this change affects Intel® Management and Security Status application behavior for the current user account only).

Note: This user selection will affect the "Intel® Management and Security Status application will be available next time I log on to Windows*" checkbox on General Tab.

3.8   Windows* 8

When the application is installed on a Windows* 8 operating system, a Windows* 8 UI tile is placed on the Windows* 8 start screen. This allows the application to send Toast* notifications to the Windows* 8 UI. If the tile is deleted, no Toast* notifications can be posted.

The application will re-create the Windows* 8 UI tile (if missing) if Intel® Active Management Technology is provisioned on the system.

§

4 Troubleshooting Intel® Management and Security Status Application

4.1 Error message appears upon application load

.NET applications fail when executed in an environment that has no Microsoft* .NET Framework installed. Microsoft* does not provide a safeguard mechanism in such conditions.

The Intel® Management and Security Status application will display the following error message if no Microsoft* .NET Framework is present in the system:

Figure 4-1.

Please install Microsoft* .NET Framework version 3.5 or above and then re-open the application.

The Intel® Management and Security Status application will not get installed if Microsoft* .NET Framework version lower than 2.0 or no Microsoft* .NET Framework version at all is installed on the system.

§

5 Intel® Management and Security Status Application Error Codes

5.1 Partial Firmware Update Failures

Intel ME Wireless LAN updates, and User Consent language updates both utilize the 'Partial Firmware Update' feature of IMSS. In the event that Partial Firmware Update failed, the user will be notified via a balloon that the update failed. The Windows* Event Log will include an error code, signifying the cause of the failure. The possible causes are listed below:

Code	Meaning
8193	Intel® ME Interface : Cannot locate Intel ME device driver
8703	PLEASE REBOOT YOUR SYSTEM. Firmware update cannot be initiated without a reboot
8704	Firmware update operation not initiated due to a SKU mismatch
8705	Firmware update not initiated due to version mismatch
8706	Firmware update not initiated due to integrity failure or invalid FW image
8707	Firmware update failed due to an internal error
8708	Firmware Update operation not initiated because a firmware update is already in progress
8710	Firmware update tool failed due to insufficient memory
8713	Firmware update not initiated due to an invalid FW image or header
8714	Firmware update not initiated due to file open or read failure
8716	Invalid usage
8718	Update operation timed-out; cannot determine if the operation succeeded

Code	Meaning
8719	Firmware update cannot be initiated because Local Firmware update is disabled
8722	Intel® ME Interface : Unsupported message type
8723	No Firmware update is happening.
8724	Platform did not respond to update request.
8725	Failed to receive last update status from the firmware.
8727	Firmware update tool failed to get the firmware parameters.
8728	This version of the Intel® FW Update Tool is not compatible with the current platform.
8741	FW Update Failed.
8744	OEM ID verification failed.
8745	Firmware update cannot be initiated because the OEM ID provided is incorrect.
8746	Firmware update not initiated due to invalid image length.
8747	Firmware update not initiated due to an unavailable global buffer.
8748	Firmware update not initiated due to invalid firmware parameters.
8754	Encountered error writing to file.
8757	Display FW Version failed.
8758	The image provided is not supported by the platform.
8759	Internal Error.
8760	Update downgrade vetoed.
8761	Firmware write file failure.
8762	Firmware read file failure.
8763	Firmware delete file failure.

Code	Meaning
8764	Partition layout NOT compatible.
8765	Downgrade NOT allowed, data mismatched.
8766	Password did not match.
8768	Password Not provided when required.
8769	Polling for FW Update Failed.
8771	Invalid File.
8772	Invalid usage, -allows v switch required to update the same version firmware.
8776	Get Partition Attribute Failure.
8777	Update Info Status Failure.
8778	Unable to read FW version from file. Please verify the update image used.
8780	Buffer Copy Failure.
8787	Password exceeded maximum number of retries.
8793	FW Update/Downgrade is not allowed to the supplied FW image.
8794	FW downgrade is not allowed due to SVN restriction.

§